PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-269272
(43)Date of publication of application : 20.09.2002

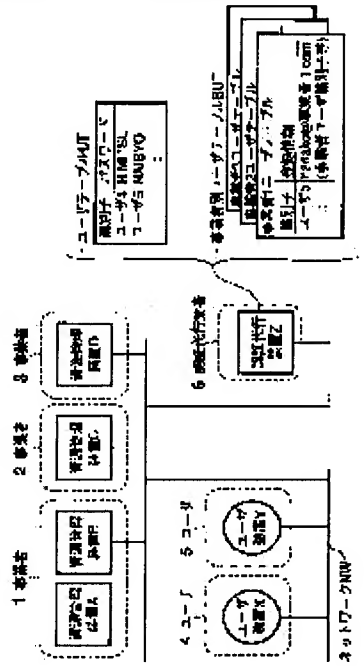
(51)Int.Cl. G06F 17/60

(21)Application number : 2001-070642
(22)Date of filing : 13.03.2001

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : SATO NAOYUKI
TAKADA SHINYA
GOTO SHINICHIRO
HANAKI SABURO

(54) AUTHENTICATION SUBSTITUTION METHOD AND APPARATUS, AUTHENTICATION SUBSTITUTION PROGRAM AND RECORD MEDIUM RECORDING THE PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an authentication substitution method capable of realizing a single sign on among a plurality of resources provided to a user by a plurality of entrepreneur estranged from each other and providing only a person himself confirming processing function to the entrepreneur.
SOLUTION: When an authentication request is received from a user device, authentication for the user is performed using the authentication information registered in a user table, and when the user is identified, according to the information on the identified user registered in a entrepreneur user table, the user device gains access to a resource management device to prepare an access certification for receiving provision of the resource, and the certification is transmitted to the user device.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－269272
（P2002－269272A）
(43)公開日　平成14年９月20日(2002.9.20)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　17/60	１４０ ５０４	Ｇ０６Ｆ　17/60	１４０ ５０４

審査請求　未請求　請求項の数４　ＯＬ　（全 ６ 頁）

(21)出願番号　特願2001－70642(P2001－70642)

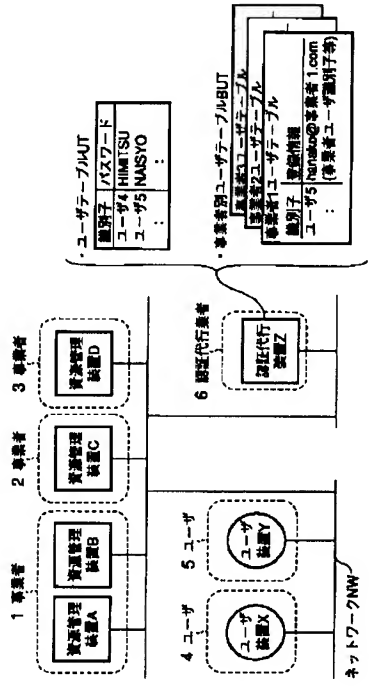
(22)出願日　平成13年３月13日(2001.3.13)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　佐藤　直之
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　高田　慎也
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100058479
弁理士　鈴江　武彦　（外２名）

最終頁に続く

(54)【発明の名称】　認証代行方法及び装置、認証代行プログラム並びにそのプログラムを記録した記録媒体

(57)【要約】
【課題】本発明の課題は、疎な関係にある複数の事業者がユーザに提供する複数の資源間でのシングルサインオンを実現し、事業者へは本人確認処理機能のみの提供を行うことを可能とする認証代行方法を提供することにある。
【解決手段】本発明は、ユーザ装置からの認証要求を受け付けると、ユーザテーブルに登録された認証情報を用いてユーザの識別を行い、ユーザを識別すると、事業者別ユーザテーブルに登録された、識別されたユーザについての情報を元に、ユーザ装置が資源管理装置にアクセスして資源の提供を受けるアクセス許可証を作成し、これをユーザ装置へ送信することを特徴とする。



1

【特許請求の範囲】

【請求項１】　ユーザ装置からの認証要求を受け付けると、ユーザテーブルに登録された認証情報を用いてユーザの識別を行うユーザ識別ステップと、

前記ユーザ識別ステップでユーザを識別すると、事業者別ユーザテーブルに登録された、識別されたユーザについての情報を元に、ユーザ装置が資源管理装置にアクセスして資源の提供を受けるアクセス許可証を作成し、これをユーザ装置へ送信するアクセス許可証作成・送信ステップとを有することを特徴とする認証代行方法。

【請求項２】　ネットワークに接続可能なインターフェイスと、

ユーザの識別を行う認証情報が登録されたユーザテーブルと、

識別されたユーザについての情報が登録された事業者別ユーザテーブルと、

ユーザ装置からの認証要求を受け付けると、ユーザテーブルに登録された認証情報を用いてユーザの識別を行うユーザ識別手段と、

ユーザを識別すると、事業者別ユーザテーブルに登録された、識別されたユーザについての情報を元に、ユーザ装置が資源管理装置にアクセスして資源の提供を受けるアクセス許可証を作成し、これをユーザ装置へ送信するアクセス許可証作成・送信手段とを具備することを特徴とする認証代行装置。

【請求項３】　ユーザ装置からの認証要求を受け付けると、ユーザテーブルに登録された認証情報を用いてユーザの識別を行うユーザ識別手順、

前記ユーザ識別手順でユーザを識別すると、事業者別ユーザテーブルに登録された、識別されたユーザについての情報を元に、ユーザ装置が資源管理装置にアクセスして資源の提供を受けるアクセス許可証を作成し、これをユーザ装置へ送信するアクセス許可証作成・送信手順をコンピュータに実行させるための認証代行プログラム。

【請求項４】　ユーザ装置からの認証要求を受け付けると、ユーザテーブルに登録された認証情報を用いてユーザの識別を行うユーザ識別手順、

前記ユーザ識別手順でユーザを識別すると、事業者別ユーザテーブルに登録された、識別されたユーザについての情報を元に、ユーザ装置が資源管理装置にアクセスして資源の提供を受けるアクセス許可証を作成し、これをユーザ装置へ送信するアクセス許可証作成・送信手順をコンピュータに実行させるための認証代行プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ユーザに何らかのサービスを提供する事業者に対して、ユーザの本人確認処理を代行するサービスを提供する認証代行業者が利用する、認証代行方法及び装置、認証代行プログラム並びにそのプログラムを記録した記録媒体に関するものである。

2

【０００２】

【従来の技術】近年、インターネット等で標準的に用いられているＷｅｂ環境における認証技術として、シングルサインオンと呼ばれる手法が提案されている。シングルサインオンとは、一度の認証処理のみで複数の資源（Ｗｅｂリソース）を利用できるようにする技術である。これによって、ユーザはＩＤとパスワードを一度入力するだけで、複数のＷｅｂサーバ上に配置されアクセス制御された資源を利用することができるようになる。ところが、現在提案されているシングルサインオンの手法の多くは、一つの事業者あるいは統合的に管理された複数の資源間において利用されることを前提に設計・構成されている。このため、インターネット等の開放型ネットワーク環境において、疎な関係にある複数の事業者が提供する資源間でシングルサインオンを実現することは難しい。

【０００３】また、現在提案されている多くの認証技術では、認証処理を構成する基本的な二つの機能、すなわちユーザを識別する本人確認処理機能（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）と確認されたユーザに対して権限を確認する権限確認処理機能（Ａｕｔｈｏｒｉｚａｔｉｏｎ）とを、別々の二つの機能として分離して取り扱っていない。一般に、本人確認処理機能については、認証を必要とする複数の資源（システム）間において、共通の要件のもとに設計・構築することが可能な機能である。

【０００４】これに対して、権限確認処理機能については、各々の事業者および資源に特有の個別の要件のもとに設計・運用される必要がある場合が多い。認証が必要な複数の資源間において、基本的な本人確認処理のみを共有することができれば、全体としてシステムの負荷は軽減する。

【０００５】

【発明が解決しようとする課題】本発明は上記の事情に鑑みてなされたもので、疎な関係にある複数の事業者がユーザに提供する複数の資源間でのシングルサインオンを実現し、各資源に対して認証処理の一部を代行し、また、本人確認処理と権限確認処理を明確に分離し、事業者へは本人確認処理機能のみの提供を行うことを可能とする、認証代行方法及び装置、認証代行プログラム並びにそのプログラムを記録した記録媒体を提供することを目的とする。

【０００６】

【課題を解決するための手段】上記目的を達成するために本発明の認証代行方法は、ユーザ装置からの認証要求を受け付けると、ユーザテーブルに登録された認証情報を用いてユーザの識別を行うユーザ識別ステップと、前記ユーザ識別ステップでユーザを識別すると、事業者別ユーザテーブルに登録された、識別されたユーザについ

ての情報を元に、ユーザ装置が資源管理装置にアクセスして資源の提供を受けるアクセス許可証を作成し、これをユーザ装置へ送信するアクセス許可証作成・送信ステップとを有することを特徴とする。

【０００７】また本発明の認証代行装置は、ネットワークに接続可能なインターフェイスと、ユーザの識別を行う認証情報が登録されたユーザテーブルと、識別されたユーザについての情報が登録された事業者別ユーザテーブルと、ユーザ装置からの認証要求を受け付けると、ユーザテーブルに登録された認証情報を用いてユーザの識別を行うユーザ識別手段と、ユーザを識別すると、事業者別ユーザテーブルに登録された、識別されたユーザについての情報を元に、ユーザ装置が資源管理装置にアクセスして資源の提供を受けるアクセス許可証を作成し、これをユーザ装置へ送信するアクセス許可証作成・送信手段とを具備することを特徴とするものである。

【０００８】また本発明の認証代行プログラムは、ユーザ装置からの認証要求を受け付けると、ユーザテーブルに登録された認証情報を用いてユーザの識別を行うユーザ識別手順、前記ユーザ識別手順でユーザを識別すると、事業者別ユーザテーブルに登録された、識別されたユーザについての情報を元に、ユーザ装置が資源管理装置にアクセスして資源の提供を受けるアクセス許可証を作成し、これをユーザ装置へ送信するアクセス許可証作成・送信手順をコンピュータに実行させるためのものである。

【０００９】また本発明の記録媒体は、ユーザ装置からの認証要求を受け付けると、ユーザテーブルに登録された認証情報を用いてユーザの識別を行うユーザ識別手順、前記ユーザ識別手順でユーザを識別すると、事業者別ユーザテーブルに登録された、識別されたユーザについての情報を元に、ユーザ装置が資源管理装置にアクセスして資源の提供を受けるアクセス許可証を作成し、これをユーザ装置へ送信するアクセス許可証作成・送信手順をコンピュータに実行させるための認証代行プログラムを記録したものである。

【００１０】

【発明の実施の形態】以下図面を参照して本発明の実施形態例を詳細に説明する。

【００１１】図１は、本発明に適した認証代行システムを示す構成説明図である。

【００１２】すなわち、複数の資源管理装置Ａ，Ｂ，Ｃ，Ｄ、複数のユーザ装置Ｘ，Ｙ、認証代行装置ＺはネットワークＮＷに接続可能なインターフェイスを持っている。前記認証代行装置Ｚは、例えば識別子、パスワード等のユーザの識別を行う認証情報が登録されたユーザテーブルＵＴ、及び識別子、登録情報等の識別されたユーザについての情報が登録された事業者別ユーザテーブルＢＵＴを持っている。前記複数の資源管理装置Ａ，Ｂ，Ｃ，Ｄ、複数のユーザ装置Ｘ，Ｙ、認証代行装置Ｚはコンピュータネットワーク ＮＷに接続されている。前記資源管理装置Ａ，Ｂは事業者１によって運営され、前記資源管理装置Ｃは事業者２によって運営され、前記資源管理装置Ｄは事業者３によって運営される。前記ユーザ装置Ｘはユーザ４によって操作され、前記ユーザ装置Ｙはユーザ５によって操作される。前記認証代行装置Ｚは認証代行業者６によって運営される。

【００１３】各ユーザ装置Ｘ，ＹにはＷｅｂブラウザがインストールされており、資源管理装置Ａ～ＤはＷｅｂサーバを介して、もしくはＨＴＴＰプロトコルを用いてＷｅｂブラウザと通信し資源をユーザ４，５へ提供する。認証代行装置ＺはＨＴＴＰプロトコル等を用いてＷｅｂブラウザと通信し本人確認処理を実施する。

【００１４】図２は、本発明の実施形態例に係るユーザ５が事業者１の資源管理装置Ａが管理している資源を利用する場合の本人確認処理における認証代行装置Ｚの処理フローを示すフローチャートである。すなわち、ユーザ５ははじめに認証代行装置Ｚに対してユーザ装置ＹのＷｅｂブラウザを用いてアクセスし、本人確認処理を行う。図２中の「本人確認を実施」のプロセスにおいて、ユーザ５はあらかじめユーザテーブルＵＴに登録してある認証情報を用いて自分の証明を行う。具体的な証明の方法としては、個人を確認するための既存のどの識別手法を採用してもよい。この手法には、パスワード（ワンタイムパスワードを含む）を用いた方法、標準規格Ｘ．５０９のような証明書を用いた方法、指紋を用いた方法、筆跡を用いた方法、ＬＤＡＰ（Ｌｉｇｈｔｗｅｉｇｈｔ　Ｄｉｒｅｃｔｏｒｙ　Ａｃｃｅｓｓ　Ｐｒｏｔｏｃｏｌ）　を利用した方法などが含まれる。もちろん、認証代行装置Ｚは、上記の二つ以上の方法に対応しこれを採用してもよい。また、今後新たな個人の識別手法が確立した場合、本プロセスの機能が拡張されることによって、この恩恵を全ユーザ・全事業者・認証代行業者が受けることができる。

【００１５】認証代行装置Ｚは、ユーザ５の識別に成功すると、登録された全ての事業者別ユーザテーブルＢＵＴを参照し当該ユーザ５についての全ての情報を抽出する。この情報には、各事業者が各々のユーザに割り当てた固有のユーザ識別子（事業者ユーザ識別子）が含まれる。認証代行装置Ｚは、これらの情報を組み込んだ一時的なアクセス許可証（Ｃｏｏｋｉｅ）を作成し、ユーザ装置ＹのＷｅｂブラウザに返信する。認証代行装置Ｚは、自身が各ユーザに割り当てた識別子をアクセス許可証（Ｃｏｏｋｉｅ）に含めてもよい。また、認証代行装置Ｚは、事業者別ユーザテーブルＢＵＴに登録された各情報について、当該事業者１の管理する資源管理装置Ａしか該当情報を導出できないようにアクセス許可証（Ｃｏｏｋｉｅ）を構成することもできる。このためには、一般的な暗号化の技術（慣用暗号、公開鍵暗号）が利用できる。図４および図５には、アクセス許可証（Ｃｏｏ

ｋｉｅ）の構成およびその作成例を示した。尚、本人確認に失敗した場合には認証失敗をユーザ５に通知する。

【００１６】図３は、本発明の実施形態例に係る権限確認処理における資源管理装置Ａの処理フローを示すフローチャートである。すなわち、ユーザ５は、アクセス許可証（Ｃｏｏｋｉｅ）を提示して、ユーザ装置ＹのＷｅｂブラウザを用いて資源管理装置Ａにアクセスする。資源管理装置Ａはアクセス許可証（Ｃｏｏｋｉｅ）から事業者別ユーザテーブルＢＵＴに登録されていた該ユーザの情報（事業者ユーザ識別子を含む）を取り出す。前述の暗号化の手法が採用されていた場合、資源管理装置Ａは、事業者１に対応した事業者別ユーザテーブルＢＵＴに登録された該ユーザ５についての情報しか取り出すことができない。資源管理装置Ａは、事業者ユーザ識別子の示すユーザ５に与えられた権限確認を実施し、権限の範囲内でユーザ５のアクセスを許し、ユーザ５に対して資源の提供を行う。事業者ユーザ識別子の示す各ユーザに対する権限の内容は、事業者１の管理者によってあらかじめ資源管理装置Ａに登録されているか、あるいは資源管理装置Ａがネットワークを介した通信等によって事業者１の管理する他の装置から即時に取得できるようにシステムが構成されている必要がある。尚、権限確認を失敗した場合には認証失敗をユーザ５に通知する。

【００１７】続けて、ユーザ５が事業者３の資源管理装置Ｄの管理する資源を利用する場合、ユーザ５はあらためて認証代行装置Ｚに本人確認処理を依頼する必要はない。ユーザが以前に獲得したアクセス許可証（Ｃｏｏｋｉｅ）には、資源管理装置Ｄのアクセスに必要な情報は含まれている。従って、ユーザ５はユーザ装置ＹのＷｅｂブラウザを用いて資源管理装置Ｄに直ちにアクセスを行い（図３の権限確認処理の実施）、資源を利用することができる。これはシングルサインオンを実現していることと等しい。

【００１８】以上の説明には詳細や特性が多く含まれるが、これらは説明のためだけであって、本発明がこれらに限定されることはない。もちろん、資源とはＷｅｂリソースだけでなく、商品・サービス等もこれに含まれる。

【００１９】尚、前記実施形態例における認証代行方法は、具体的にはパソコン等のコンピュータにより、予め＊所定の認証代行プログラムに基づいて実行される。前記認証代行プログラムは所定のコンピュータ読み取り可能な記録媒体に記録することができる。

【００２０】すなわち、前記認証代行プログラムは、ユーザ装置からの認証要求を受け付けると、ユーザテーブルに登録された認証情報を用いてユーザの識別を行うユーザ識別手順、前記ユーザ識別手順でユーザを識別すると、事業者別ユーザテーブルに登録された、識別されたユーザについての情報を元に、ユーザ装置が資源管理装置にアクセスして資源の提供を受けるアクセス許可証を作成し、これをユーザ装置へ送信するアクセス許可証作成・送信手順をコンピュータに実行させる。

【００２１】

【発明の効果】以上述べたように本発明によれば、互いに疎な関係にある複数の事業者が提供する複数の資源間でのシングルサインオンを実現する認証代行装置を容易に構築できる。また、本人確認処理と権限確認処理を明確に分離しており、認証代行装置を運営する事業者は、ユーザへ資源（商品・サービスを含む）を提供する事業者に対して、本人確認処理機能のみを提供することを可能とする。

【図面の簡単な説明】

【図１】本発明の実施形態例に係る認証代行システムを示す構成説明図である。

【図２】本発明の実施形態例に係る本人確認処理における認証代行装置の処理フローを示すフローチャートである。

【図３】本発明の実施形態例に係る権限確認処理における資源管理装置の処理フローを示すフローチャートである。

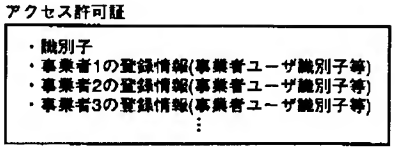
【図４】本発明の実施形態例に係るアクセス許可証を示す構成説明図である。

【図５】本発明の実施形態例に係るアクセス許可証の作成例を示す説明図である。

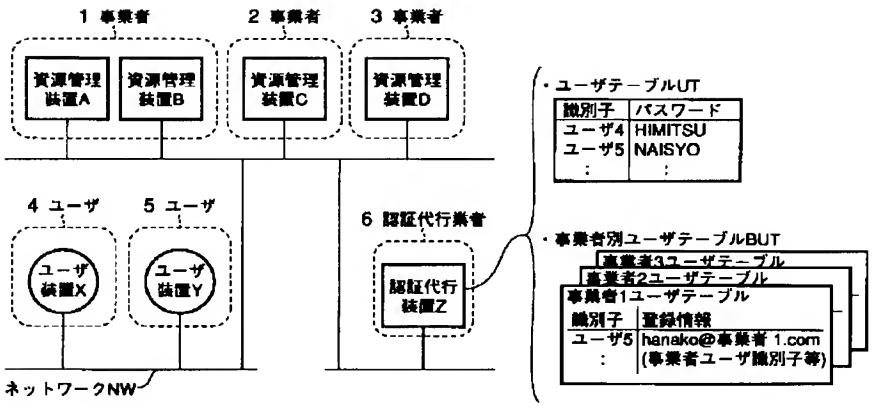
【符号の説明】

Ａ～Ｄ　資源管理装置
Ｘ，Ｙ　ユーザ装置
Ｚ　認証代行装置
ＵＴ　ユーザテーブル
ＢＵＴ　事業者別ユーザテーブル

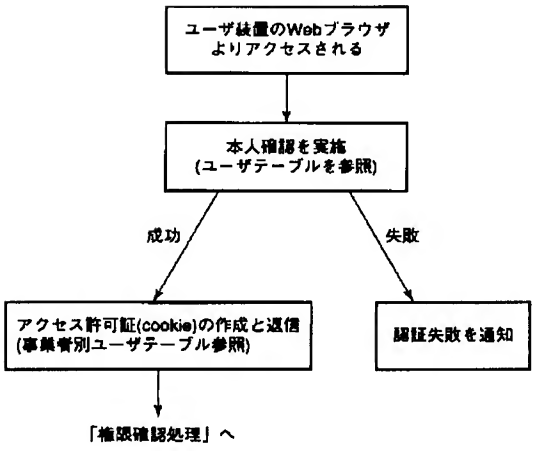
【図４】



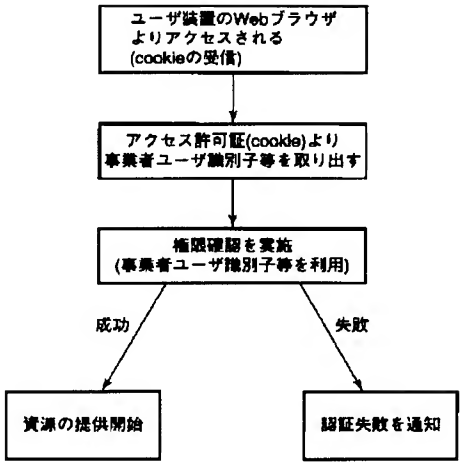
【図１】


1 事業者
2 事業者
3 事業者
資源管理装置A
資源管理装置B
資源管理装置C
資源管理装置D
4 ユーザ
5 ユーザ
ユーザ装置X
ユーザ装置Y
6 認証代行業者
認証代行装置Z
ネットワークNW
・ユーザテーブルUT
識別子 パスワード
ユーザ4 HIMITSU
ユーザ5 NAISYO
・事業者別ユーザテーブルBUT
事業者3ユーザテーブル
事業者2ユーザテーブル
事業者1ユーザテーブル
識別子 登録情報
ユーザ5 hanako@事業者1.com
(事業者ユーザ識別子等)

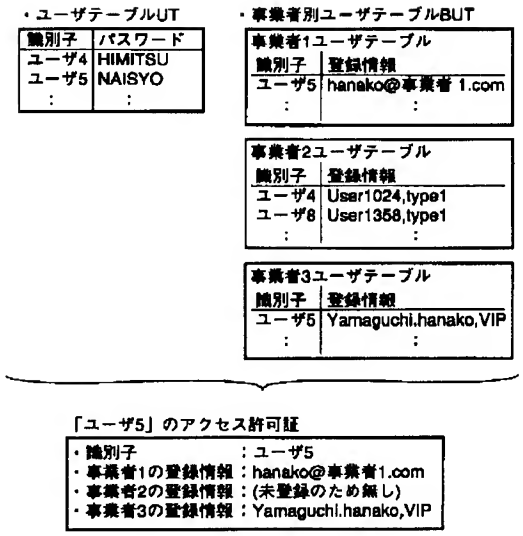
【図２】


ユーザ装置のWebブラウザよりアクセスされる
本人確認を実施(ユーザテーブルを参照)
成功
失敗
アクセス許可証(cookie)の作成と返信(事業者別ユーザテーブル参照)
認証失敗を通知
「権限確認処理」へ

【図３】


ユーザ装置のWebブラウザよりアクセスされる(cookieの受信)
アクセス許可証(cookie)より事業者ユーザ識別子等を取り出す
権限確認を実施(事業者ユーザ識別子等を利用)
成功
失敗
資源の提供開始
認証失敗を通知

【図５】



フロントページの続き

(72)発明者　後藤　真一郎
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

(72)発明者　花木　三良
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内